**UCL GDPR Programme**

**Email Guidance Note**

**Introduction**

This guidance has been produced to help you to ensure the proper and efficient use of UCL’s email service. Following these recommendations helps UCL comply with new data protection legislation and assists you to manage your email more effectively.

UCL’s Email Policy is currently being updated in light of the new legislation. Until the update is complete, this guidance note serves to introduce some principles around good email management practice.

**1] Whether to keep the email messages**

Deciding whether or not to keep emails can be difficult. Whilst it may feel necessary to keep a record of all correspondence in case you need to refer back to it, much of what is kept will often not be needed and will only clutter your inbox.

If email messages contain important information, it is often good practice to save this elsewhere, such as on a UCL shared drive or in SharePoint.

Try to get into the habit of reviewing email messages regularly - deleting any working copies, trivial emails, out-of-date reference material and duplicates to prevent material taking up unnecessary space. You can use the [auto-archive and auto-delete functions within Outlook](https://support.office.com/en-us/article/archive-in-outlook-2016-for-windows-25f75777-3cdc-4c77-9783-5929c7b47028) to stop your inbox from getting out of control. It is good practice to manage your emails into folders and generally try to keep emails in your inbox to a minimum.

UCL’s [**Retention Schedule**](https://www.ucl.ac.uk/library/docs/retention-schedule.pdf) provides further guidance on the disposal and storage of email records.

**2] Use CC & BCC with care**

Every time a message containing personal data is copied to another recipient there is an increased information compliance risk. Limit the use of CC only to those who need to receive the information. Where you regularly have to send personal information, use alternative sharing tools such as Sharepoint and OneDrive [see below].

With the above in mind where it is still necessary to send to multiple recipients BCC can be a useful tool. BCC (Blind Carbon Copy) is a means of sending an email to a large number of people without them knowing who else is getting the email.

Case study: Gloucester Constabulary were recently fined £80,000 by the ICO for sending a bulk email that identified victims of non-recent child abuse. Use of the BCC function in this case would have prevented their details from being seen by others.

**3] Consider using encryption**

Caution should always be exercised when sending emails containing personal data, e.g. spreadsheets with a large amount of personal data. The risks of transferring personal data increase when emailing non-UCL recipients, i.e. those not using an “@UCL” email addresses. Robust encryption is recommended as it can be used to ensure confidentiality. Encryption keeps data private by converting it to an unreadable format. Only people who have an encryption key can access the data.

Please refer to the ISD-produced [guidance on options for encryption](https://www.ucl.ac.uk/informationsecurity/itsecurity/knowledgebase/securitybaselines/encryption/email-encryption) for more information. If you are uncertain about how best to utilise encryption, please seek advice from the isg@ucl.ac.uk.

**4] Is there a better way of sharing information?**

Using email for sharing documents and personal information is often not the best method. Sharepoint and One Drive are both secure features of Office 365 as offered by UCL.

[Sharepoint](https://www.ucl.ac.uk/isd/services/communicate-collaborate/sharepoint-and-onedrive-for-business) is a web-based collaboration space which can be used to create, edit and share content between colleagues. There are a number of different service levels offered by UCL depending on business use and your skill level. You can [contact ISD to request your own Sharepoint site.](https://liveuclac.sharepoint.com/sites/SharePoint/SitePages/Requests.aspx)

OneDrive for Business is a web-based collaboration space designed for personal use, such as sharing a file with an individual. UCL staff and students are each allocated 1TB of storage space for [OneDrive](https://www.ucl.ac.uk/isd/services/communicate-collaborate/sharepoint-and-onedrive-for-business).

UCL’s shared drive provides access according to file system permissions. It is secure and is backed up on a daily basis.

**5] Use generic/shared role accounts and shared mailboxes**

A role account is a generic user ID assigned for one specific role that can be used by more than one person. The account must have a registered owner. Role accounts can only be used by one person at a time and must not be used for personal email or file storage. They will have access to an email address, N:\ storage, Desktop@UCL and Eduroam, but not to print@UCL or library services.

Use of role accounts must be reviewed annually to ensure continued need. If no longer needed this must be relayed back to User Services by filling in the [self-service form](https://ucl.my.salesforce.com/?startURL=/apex/bmcservicedesk__ssredirect?type=sr%26id=a3S20000000LDPdEAO) so the role account can be closed.

If you wish to use a role account for email collaboration, you should use a [shared mailbox](https://www.ucl.ac.uk/isd/services/email-calendar/collaborate/shared-mailboxes). This allows for multiple access to a single mailbox, useful for a number of circumstances such as the ability for a PA to access a manager’s inbox.

**6] Use an Out of Office message**

Out of Office (OOO) should be used in all cases where staff are away/unable to access their email. The OOO message should include dates of no email access, and alternative contact details – a mailbox or a colleague who may be able to assist the sender.

Please see the UCL [guidance on out of office messages](https://www.ucl.ac.uk/legal-services/ucl-general-data-protection-regulation-gdpr/guidance-notices-ucl-staff/guidance-note-out-office).

**7] Tips on content**

Be objective and professional. Bear in mind that emails are subject to ‘access to information regimes’, i.e. freedom of information and data protection legislation – what you write in an email may have to be disclosed.

One subject per message: Limit the content in each email message to one subject, which will make management easier. Keep subject lines concise, clear and related to the purpose of the email. They should avoid personal data.

Establish email protocols in your local areas to ensure that everyone in your office manages their email in a similar way.

**8] Using folders**

Use folders to manage your email. For example, use a folder called ‘private and personal’ that clearly indicates the nature of the messages to be stored.

**9] Further reading**[Email Policy](https://www.ucl.ac.uk/informationsecurity/policy/public-policy/policy-on-electronic-mail.pdf)[Information Security Policy](https://www.ucl.ac.uk/informationsecurity/policy)
[Retention Schedule](http://www.ucl.ac.uk/library/about/records-office/retention)
[Computing Regulations](https://www.ucl.ac.uk/informationsecurity/policy/public-policy/Computing-Regulations-Acceptable-Use-Policy-0117.pdf)
[Guidance on mailing lists](https://www.ucl.ac.uk/legal-services/ucl-general-data-protection-regulation-gdpr/guidance-notices-ucl-staff/guidance-note-actions-take)